PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-093557

(43)Date of publication of application : 10.04.1998

(51)Int.Cl. H04L 12/24
H04L 12/26
H04B 17/00
H04L 12/56
H04L 29/14

(21)Application number : 08-243285

(22)Date of filing : 13.09.1996

(71)Applicant : TOSHIBA CORP

(72)Inventor : KATO TAKEHISA
SHIMIZU HIDEO
KITAORI MASASHI
KAWAMURA SHINICHI
ENDO NAOKI

(54) COMMUNICATION MONITOR DEVICE AND COMMUNICATION MONITOR METHOD

(57) [Abstract]

[PROBLEM TO BE SOLVED] To provide an encryption communication system enabling efficiently and effectively monitoring a content of encrypted information transmitted from an internal network to an external network.

[SOLUTION] A communicator monitor that monitors encrypted information transmitted from a terminal belonging to an internal network to be a managing target to a terminal connected via an external network, concerning information transmitted from the terminal belonging to the internal network to the terminal connected via the external network, is characterized in having a means for collecting a transmission history with a pair of a transmission source and a transmission destination as a key and a means for not transferring the information to the transmission destination and transferring to a predefined specific address when transmitting the information possessed by the pair of the transmission source and the transmission destination for which a prescribed statistic amount obtained by the collected transmission history has satisfied a prescribed condition.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－93557

(43)公開日　平成10年(1998)４月10日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　12/24		Ｈ０４Ｌ	11/08	
12/26		Ｈ０４Ｂ	17/00	Ｚ
Ｈ０４Ｂ　17/00		Ｈ０４Ｌ	11/20	１０２Ｚ
Ｈ０４Ｌ　12/56			13/00	３１３
29/14				

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平8－243285

(22)出願日　平成８年(1996)９月13日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　加藤　岳久
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　清水　秀夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　北折　昌司
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　弁理士　鈴江　武彦　（外６名）

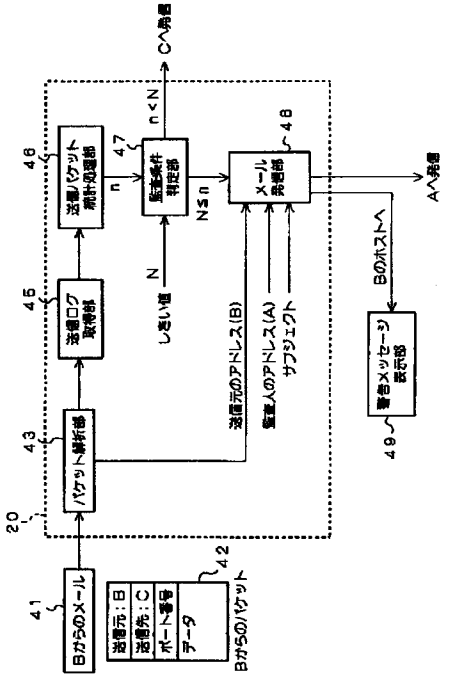
最終頁に続く

(54)【発明の名称】　通信監査装置及び通信監査方法

(57)【要約】

【課題】　内部ネットワークから外部ネットワークへ送り出される暗号化された情報の内容の監視を効率的かつ効果的に行うことのできる暗号通信システムを提供すること。

【解決手段】　管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報を監視する通信監査装置において、前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向けて送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集する手段と、収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった送信元と送信先の組を持つ情報が送信されようとする場合、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送する手段とを備えたことを特徴とする。



1

【特許請求の範囲】

【請求項１】管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報を監視する通信監査装置において、

前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向けて送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集する手段と、

収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった送信元と送信先の組を持つ情報が送信されようとする場合、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送する手段とを備えたことを特徴とする通信監査装置。

【請求項２】前記外部ネットワークを介して接続された端末を送信先とする情報を復号して内容を監査する場合がある旨の警告文を、所定のタイミングで前記内部ネットワークに属する端末に表示させる手段を備えたことを特徴とする請求項１に記載の通信監査装置。

【請求項３】前記転送する手段により前記情報が前記特定の宛先に転送される場合に、該情報を該送信先に転送せずに復号して内容を監査する旨のメッセージを、該情報を発した送信元の端末に送信する手段を備えたことを特徴とする請求項１に記載の通信監査装置。

【請求項４】管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報を監視する通信監査方法において、

前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向けて送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集し、

収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった送信元と送信先の組を持つ情報が送信されようとする場合、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送することを特徴とする通信監査方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続された端末間で情報を暗号化して送受信する暗号通信システムに関する。

【０００２】

【従来の技術】近年では、ネットワークに接続されたワークステーションやパーソナルコンピュータなどの端末間で文書・画像・音声などの情報を電子化して送受信する通信システムが広く普及している。

【０００３】このような通信システムにおいて、情報の受け渡しにあたっては（特に外部のネットワークを介した情報の受け渡しにあたっては）、情報の秘匿性を確保するために、送信側で情報を暗号化し、受信側で暗号化された情報を復号する暗号通信を用いることが多い。すなわち、情報を暗号化してネットワークへ送信することで、送信者が宛先として指定した相手以外のネットワーク利用者にはその情報を閲覧等することができなくなり、情報の秘匿性を保つことができる。

2

【０００４】しかしながら、ある一纏まりのネットワーク（例えば社内ネット）からその外部へ送り出される情報について、その情報が例えば企業秘密に関わる情報であるか否かなどについて監視しようしても、その送り出されようとする情報を逐一復号する必要があり、監視が困難であった。

【０００５】

【発明が解決しようとする課題】以上のように従来は、ネットワークを用いて暗号化された情報の受け渡しを行う通信システムにおいて、ある一纏まりのネットワークからその外部へ送り出される情報の内容を監視することが困難であった。

【０００６】本発明は、上記事情を考慮してなされたもので、ネットワークを用いて暗号化された情報の受け渡しを行う通信システムにおいて、ある一纏まりのネットワークからその外部へ送り出される情報の内容の監視を効率的かつ効果的に行うことのできる暗号通信システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明（請求項１）は、管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報（例えば、文書、画像、音声など）を監視する通信監査装置において、前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向けて送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集する手段と、収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった（例えば、総転送回数がしきい値を越えるものとなった）送信元と送信先の組を持つ情報が送信されようとする場合、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送する手段とを備えたことを特徴とする。

【０００８】これによって、前記情報の転送を受けた前記特定の宛先の端末を操作可能な監査人は、送信元ユーザ（または送信元ユーザと送信先ユーザの組）により特定される復号鍵を用いて該情報を復号して内容を監査することができる。

【０００９】また、監査後、その内容に問題がないと判断された場合には、該特定の端末から情報をあらためて送信先に向けて送り出すようにしても良い。あるいは、通信監査装置内に該パケットを識別子を付して保持しておき、該特定の端末から通信監査装置にパケットの識別

子を指定して該パケットをその本来の送信先に向けて送り出すよう指示を出すようにしても良い。あるいは、該情報の送信元に該情報を再度その本来の送信先に向けて送り出すよう指示を出すようにしても良い。

【００１０】ここで、前記所定の条件を適宜設定することにより、監査対象を絞った効率的かつ効果的な監査を行うことができる。例えば、所定の条件を総転送回数のしきい値とすることにより、転送回数が際だって多い特定の送信元と送信先の組を持つ情報についてのみ監査対象とすることができる。

【００１１】好ましくは、前記外部ネットワークを介して接続された端末を送信先とする情報を復号して内容を監査する場合がある旨の警告文を、所定のタイミングで（例えば該端末を立ち上げる際に）前記内部ネットワークに属する端末に表示させる手段を備えても良い。

【００１２】これによって、該端末のユーザに警告を与え、例えば外部に企業秘密に関わる情報を漏洩するような不正を未然に防止する効果を得ることができる。好ましくは、前記転送する手段により前記情報が前記特定の宛先に転送される場合に、該情報を該送信先に転送せずに復号して内容を監査する旨のメッセージを、該情報を発した送信元の端末に送信する手段を備えても良い。

【００１３】これによって、該端末のユーザは、情報が送信先に転送されなかった理由が、ネットワーク上の通信エラーなどによるものではなく、監査によるものであることを知ることができる。

【００１４】本発明（請求項４）は、管理対象となる内部ネットワークに属する端末から外部ネットワークを介して接続された端末に送信される暗号化された情報を監視する通信監査方法において、前記内部ネットワークに属する端末から前記外部ネットワークを介して接続された端末へ向けて送り送信される情報について、送信元と送信先の組をキーとして送信履歴を収集し、収集された前記送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった送信元と送信先の組を持つ情報が送信されようとする場合、該情報を該送信先に転送せずに、予め定められた特定の宛先に転送することを特徴とする。

【００１５】好ましくは、前記外部ネットワークを介して接続された端末を送信先とする情報を復号して内容を監査する場合がある旨の警告文を、所定のタイミングで前記内部ネットワークに属する端末に表示させるようにしても良い。

【００１６】好ましくは、前記転送する手段により前記情報が前記特定の宛先に転送される場合に、該情報を該送信先に転送せずに復号して内容を監査する旨のメッセージを、該情報を発した送信元の端末に送信するようにしても良い。なお、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【００１７】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。図１は、本発明の一実施形態に係る暗号通信システムを示す概念図である。図１において、内部ネットワーク１１は、社内ネットワーク（企業内ネットワーク）などのローカルエリアネットワークであり、例えば会社の各部署や工場、営業所などに設置された各端末を結んでいる。なお、内部ネットワーク１１は、社内ネットワークに限らず、所定の組織単位あるいは管理単位のネットワークであれば良い。

【００１８】外部ネットワーク１２は、内部ネットワーク１１からみた外部のネットワークである。内部ネットワークを社内ネットワークとすると、外部ネットワークは社外ネットワークに相当する。外部ネットワーク１２の一例としては、世界中に張り巡らされているインターネットが代表的である。

【００１９】情報監査装置１３は、内部ネットワーク１１に属する端末を管理対象とし、内部ネットワーク１１に属する端末から社外ネットワーク１２に送り出される情報を監視する。本実施形態では、情報をパケット単位で監視するものとする。すなわち、情報監査装置１３は、パケット内に書き込まれた送信元と送信先の情報をもとに、該パケットが内部のどのユーザを送信元とし外部のどのユーザを送信先として送り出されたかを監視し、その統計情報を収集する。そして、この統計情報をもとにパケットの監査を行う。

【００２０】図２に、本実施形態で転送対象となるパケットの一例としてＴＣＰ／ＩＰパケットの構造を示す。図２に示すように、パケットには、少なくとも、送信元のアドレス２１、送信先のアドレス２２、プロトコルの種類（ポート番号）２３、データの内容２４が含まれるものとする。

【００２１】なお、本実施形態では、パケット内に送信元となるユーザ（内部のユーザ）を特定可能なデータが含まれているものとする。例えば、送信元のアドレス２１で内部のユーザを特定可能とする。

【００２２】本実施形態では、内部のユーザは秘密鍵暗号を用いて情報（図２ではデータの内容２４）を暗号化し通信を行うものとする。内部のユーザの使用する秘密鍵は、ユーザをキーとしてあるいはユーザとその送信相手の組をキーとして、内部ネットワーク１１内で管理されているものとする。秘密鍵暗号については、池野、小山共著「現代暗号理論」電子情報通信学会編や、岡本著「暗号理論入門」共立出版株式会社等に詳しいので、ここでの説明は省略する。

【００２３】次に、通信監査装置２０の機能について説明する。通信監査装置２０は、内部のユーザから外部への送信の状況を、パケットの送信元アドレス２１と送信先アドレス２２を参照して統計的処理により把握する。そして、所定の統計量が予め定められた所定の条件を満

たすものになると（例えば転送パケットの累計数がしきい値以上になると）、パケットをその本来の送信先へは転送せずに、パケット内の暗号化された情報を復号しその内容の監査を行うために該パケットを監査人（すなわち、内部の特定のユーザ）宛てに転送する。

【００２４】以下、具体例として発信された電子メールを監査する場合について説明する。図３に、通信監査装置２０による監査の概要を示す。図３において、ユーザＡを監査人、ユーザＢを内部のユーザ（例えば社員）とし、ユーザＣとユーザＤが外部のユーザ（例えば社外のユーザ）であるとする。

【００２５】通信監査装置２０は、内部のユーザＢから外部のユーザＣ宛てあるいはユーザＤ宛てのパケットを受け取ると、パケット内に記述されている送信元アドレスと送信先アドレスを調べ、送信元と送信先の組ごとにパケット量を累計して行く。

【００２６】図３では、ユーザＢの通信記録として、Ｃ宛てにｘ回、Ｄ宛てにｙ回、パケット転送が行われた状態が示されている。ここで、例えば、上記所定の条件を「今受け取ったパケットをその宛先に転送すると通信回数がｘ（ここでｘ＞ｙとする）回を越える」条件であるとする。この場合、図３の状態でユーザＢからＤ宛てにパケットが送信されると、該パケットはこの条件を満たさないので、通信監査装置２０はＤ宛てにパケットを送り出す（Ｄ宛ての通信回数はｙ＋１となる）。一方、図３の状態でユーザＢからＣ宛てに送信されたパケットが通信監査装置２０に入力されると、Ｃ宛ての通信回数はｘ＋１にカウントアップされ、この結果、該パケットは上記条件を満たすことになるので、通信監査装置２０は、該パケットをＣ宛てには転送せずに、監査人Ａの端末宛てに転送する。

【００２７】このようにして上記パケットを転送された監査人Ａは、送信元アドレス（または送信元アドレスと送信先アドレスの組）により特定される秘密鍵を用いて該パケット内の暗号化データを復号して内容を監査することができる。なお、該秘密鍵は、監査人Ａの端末あるいはこれに直接接続されたサーバあるいは内部ネットワーク１１内の他のサーバ装置で管理し、監査人Ａの端末にて入手可能であるものとする。

【００２８】また、監査後、その内容に問題がないと判断された場合には、該監査人Ａの端末からパケットをあらためて本来の送信先に向けて送り出すようにしても良い。あるいは、通信監査装置２０内にて該パケットを識別子を付して保持しておき、該監査人Ａの端末から通信監査装置２０にパケットの識別子を指定して該パケットをその本来の送信先に向けて送り出すよう指示を出すようにしても良い。あるいは、該パケットの送信元に該パケットを再度その本来の送信先に向けて送り出すよう指示を出すようにしても良い。

【００２９】ここで、前記所定の条件を適宜設定することにより、監査対象を絞った効率的かつ効果的な監査を行うことができる。例えば、所定の条件を総転送回数のしきい値とすることにより、転送回数が際だって多い特定の送信元と送信先の組を持つ情報についてのみ監査対象とすることができる。

【００３０】次に、図４に、通信監査装置２０の内部構成の一例を示す。また、図５に、通信監査装置２０の処理の流れの一例を示す。通信監査装置２０は、パケット解析部４３、送信ログ取得部４５、送信パケット統計処理部４６、監査条件判定部４７、メール発信部４８を備えている。

【００３１】図４において、４１はユーザＢからの暗号メールを示し、４２は送信されるパケットに含まれる情報の概略を示している。まず、暗号メールを受信すると、パケット解析部４３でパケット内に記述された該パケットの送信元と送信先を検出する（ステップＳ１１）。また、必要に応じて、プロトコルの種類、データ量など、他の情報も検出する。

【００３２】次に、送信ログ取得部４５は、パケットの送信元と送信先の組ごとにログを取る。ログの内容は、例えば、日時、送信元、送信先、プロトコルの種類などからなる。あるいは、データ量などを付加しても良い。

【００３３】次に、送信パケット統計処理部４６は、送信ログ取得部４５からの情報をもとに、パケット毎に統計処理を行う（ステップＳ１２）。ここでは、送信元と送信先の組ごとにパケット数を計数するものとする。なお、送信元と送信先とプロトコルの種類の組ごとに統計処理を行っても良いし、特定の種類のプロトコルについてのみ、送信元と送信先の組ごとにパケット数の計数するようにしても良いし、その他、種々の統計処理の方法が考えられる。

【００３４】なお、送信ログ取得部４５を設けない構成も考えられる。この場合、パケット解析部４３から直接、送信パケット統計処理部４６に、必要なデータを与える。次に、監査条件判定部４７は、パケット毎に行った統計処理により得られる所定の統計量が、予め定めた条件を満たすか否か判定する（ステップＳ１３）。

【００３５】ここでは、一例として、所定の統計量を送信回数ｎとし、予め定めた条件を「送信回数ｎがしきい値Ｎ以上であること」とする。この場合、監査条件判定部４７は、暗号メールを監査するか否かを決定するためのしきい値Ｎと送信回数ｎを比較する。

【００３６】上記条件が満たされない場合（本具体例ではＮ＞ｎである場合）には（ステップＳ１４）、監査すべき条件が満たされないので、該電子メールを本来の送信先に向けて外部ネットワーク１２に送り出す（ステップＳ１５）。

【００３７】一方、上記条件が満たされる場合（本具体例ではＮ≦ｎである場合）には（ステップＳ１４）、監査すべき条件が満たされるので、メール発信部４８は、

このメールを監査人Ａに発信する（ステップＳ１６）。

【００３８】なお、通信監査装置２０内では、パケットを送信するまでバッファに蓄積しておいても良いし、パケット解析部４３、送信ログ取得部４５、送信パケット統計処理部４６、監査条件判定部４７、メール発信部４８の各部分でリレーして言っても良い。

【００３９】以下、具体例を用いて通信監査装置２０の動作例を説明する。今、図３のユーザＢが暗号メールをユーザＣ宛てに送信したとする。ユーザＢが発信した暗号メールは、パケットとして図４中の４２に示すように発信元および発信先がヘッダとして付加される。

【００４０】このパケットを受け取った通信監査装置２０では、パケット解析部４３により該パケットがユーザＢからのパケットであることと、該パケットがユーザＣへ発信されていることなどを検出し、その結果を送信ログ取得部４５へ送る。

【００４１】送信ログ取得部４５は、送信元と送信先とを組にして、パケット送信のログを記録しておく。本具体例では、ユーザＢがパケットをユーザＣに送信したログを記録しておく。

【００４２】この結果を、送信パケット統計処理部４６へ送り、ある特定のパケット、例えば現在送信されているパケットのこれまでの個数をカウントする。この結果を、ｎとする。

【００４３】このｎを監査条件判定部４７へ送り、あるしきい値Ｎと比較する。このしきい値は、監査人Ａが予め設定した値である。このとき、ｎがしきい値Ｎ未満である場合は、該パケットをユーザＣに向けて外部ネットワーク１２に送り出す。

【００４４】一方、ｎがしきい値Ｎ以上となった場合は、メール発信部４８にて、ユーザＢが送信した暗号メールを監査人Ａへ送信する。なお、同時に、ユーザＢからユーザＣへのパケットの量がしきい値Ｎ以上となったことをメールにて知らせるようにしても良い。

【００４５】この結果、監査人Ａは、ユーザＢから出されたユーザＣ宛ての暗号メールを、所定の鍵で復号し内容を監査することができる。また、メール発信部４８は、ある特定の内容を持つパケット、例えば使用されていないポート番号を付加したパケットをユーザＢのホストマシンへ送信する。ユーザＢのホストマシンは、警告メッセージ発信部４９でこの特定のパケットを受け取り、警告メッセージをユーザＢが使用しているマシンのディスプレイ上に、例えば、「これより暗号化されたメールの監査を行います」というメッセージとして表示するようにしても良い。この警告メッセージは、現在使われているファイアウォールの警告システムと同様に、各ホストマシンにソフトウェアで実現可能である。

【００４６】なお、以上では、所定の統計量としてパケット数、所定の条件として「パケット数がしきい値以上になること」を一例として示したが、これに限定されるものではない。

【００４７】例えば、監査対象とする送信元の範囲、あるいは送信先の範囲、あるいは送信元と送信先の組の範囲を限定しても良い。また、上記所定の条件あるいは所定の統計量および所定の条件を、送信元、あるいは送信先、あるいは送信元と送信先の組ごとに設定しても良い。

【００４８】また、上記所定の統計量を一定期間毎に求めても良い。例えば、転送パケット数を月初めにクリアし、当該月における転送パケット数としきい値を比較するようにしても良いし、その日から過去一定期間の間の転送パケット数で比較するようにしても良い。

【００４９】その他、種々変形して実施可能である。なお、以上では、監査するパケットを監査人に転送していたが、その代わりに、パケットは監査人に転送せずに、監査人にメッセージのみ転送するようにしても良い。この場合にも、監査人は、通信監査装置内に保持されているパケットを監査することができる。

【００５０】ところで、内部のユーザが、自分のホストマシンを立ち上げ、マシンにログインをすると、画面上に、例えば「本システムを使用して外部へ情報を暗号化して送信する場合、復号して情報の内容を監査することがあります。」というメッセージを表示させるようにしても良い。

【００５１】これによって、該端末のユーザに警告を与え、例えば外部に企業秘密に関わる情報を漏洩するような不正を心理的に抑え未然に防止する効果を得ることができる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００５２】

【発明の効果】本発明によれば、ネットワークを用いて暗号化された情報の受け渡しを行う通信システムにおいて、送信履歴をもとにして一定の条件を成立させる情報を監査対象として選択することで、内部ネットワークからその外部へ送り出される情報の内容の監視を効率的かつ効果的に行うことができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る暗号通信システムの概念を示す図

【図２】同実施形態におけるパケットの構造の一例を示す図

【図３】同実施形態の通信監査装置の動作を説明するための図

【図４】同実施形態の通信監査装置の内部構成の一例を示す図

【図５】同実施形態の通信監査装置の処理の流れの一例を示すフローチャート

【符号の説明】

１１…社外ネットワーク

9

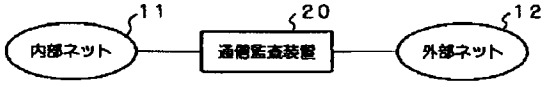
１２…社内ネットワーク
１３…通信監査装置
３５…通信監査装置
４３…パケット解析部
４５…送信ログ取得部

10

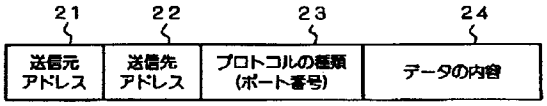
＊４６…送信パケット統計処理部
４７…監査条件判定部
４８…メール発信部
４９…警告メッセージ表示部

＊

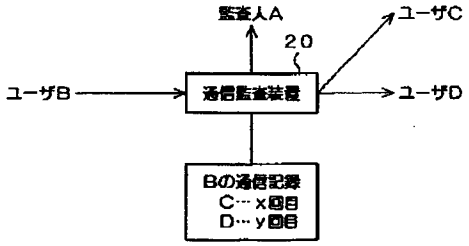
【図１】



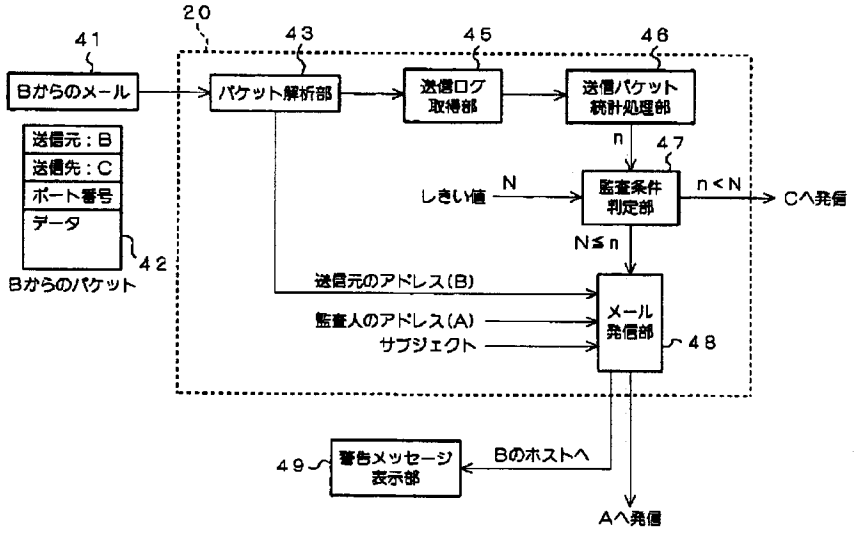
【図２】



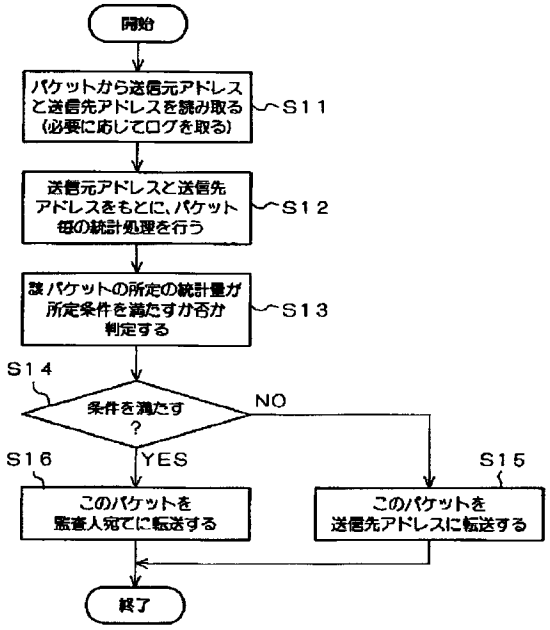
【図３】



【図４】



【図５】



フロントページの続き

(72)発明者　川村　信一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　遠藤　直樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内